The Framework of Consensus Equilibria for Blockchain Ecosystems in Fintech

George Xianzhi Yuan
Shanghai Lixin University of Accounting and Finance, Shanghai 201209 China
Business School, Chengdu University, Chengdu 610106 China
Center for Financial Engineering, Soochow University, Suzhou 215008 China, and
Business School, Sun Yat-Sen University, Guangzhou 510275 China
E-mail: george_yuan99@yahoo.com

Abstract The goal of this paper is to establish the general framework of consensus equilibria for Mining-Pool Games in Blockchain Ecosystems, and in particular to explain the stable in the sense for the existence of consensus equilibria related to mining gap game's behaviors by using one new concept called "consensus games (CG)" in Blockchain Ecosystems, here, the Blockchain ecosystem mainly means the economic activities by taking into the account of three types of different factors which are expenses, reward mechanism and mining power for the work on blockschain by applying the key consensus called "Proof of Work" due to Nakamoto in 2008.

In order to do so, we first give an outline how the general existence of consensus equilibria for Mining-Pool Games is formulated, and then used to explain the stable for Gap Games for Bitcoin in the sense by the existence of consensus equilibria under the framework of Blockchain consensus, we then establish a general existence result for consensus equilibria of general mining gap games by using the profit functions for miners as the payoffs in game theory. As applications, the general existence results for consensus equilibria of Gap games are established, which not only help us to claim the existence for the general stability for Gap games under the general framework of Blockchain ecosystems, but also allow us to illustrate a number of different phenomenons on the study of mining-pool games with possible impacts due to miners' gap behaviors with scenarios embedded in Bitcoin economics. Our study on the explanation for the stability of mining gap game for Blockchain ecosystems shows that the concept of consensus equilibria may play a important role for the development of fundamental theory for consensus economics.

Keywords: Consensus equilibrium, Nakamoto consensus, Proof of work, Stability, Blockchain ecosystems, Mining-pool game, Mining gap games, Longest chain rules (LCR), Incentive compatibility, Cooperative and non-cooperative games, Hybird solution.
JEL: C73, D82, D89, G20, G28, G39, L13, L86, O31.

1 Introduction

In the Bitcoin world, all miners following the so-called Nakamoto's consensus protocol, introduced in year 2008, and work in a number of different groups (pools) to mine for Bitcion. Work on the block in a process called "mining" is successfully and approved due to the majority of miners applying key consensus called "Proof of Work", as each miner or pool may work in different ways, we need to thus deal with the so-called "Pool-Games" of miners (also use the term, "Mining Pool Game") with their working (mining) behaviors as an individual or in a group (pool) by following either cooperative or non-cooperative ways. In order to so do, we will introduce a new notion called "Consensus Games" which will be used to establish the general existence of consensus equilibria for consensus games to describe mining behavior for Blockchain Ecosystems in Fintech. In particular, we will focus on the general discussion for the mechanism of the phenomenon called " Mining Gap Behavior " (in short, "Gap Games") for miners under the framework of general incentives consensus in which miners would avoid mining blocks when the available fees are insufficient (in particular, if incentives come only from fees, then a mining gap behavior would happen, for more in details, see Carlesten et al.(2016), Tsabary and Eyal (2018) and related references wherein).

In game theory, we know that Nash equilibrium follows the non-cooperative idea, while the concept of Core is defined by considering the cooperative behavior of players. Generally speaking, a cooperative solution concept (α-core) was first introduced by Aumann (1961). Later Scarf (1971) proved an nonemptiness result for the α-core in a normal-form game with continuous quasiconcave payoff functions.Inspired by Scarf (1971), Kajii (1992) provided a generalization of Scarf (1971) concerning games with nonordered preferences; his result and proof technique is also a modification and development by Border (1984). On the other hand, Florenzano (1989) defined the group preferences of each coalition and gave the proof by using Gale and Mas-Colell fixed point theorem. Following Florenzano's method (1989), Lefebvre (2001) provided a generalization to an economy with different information. Building on Kajii (1992), Martins-da-Rocha and Yannelis (2011) extended his result to games on (Hausdorff) topological vector spaces. For more work on the α-core, we refer to Askoura (2011), Askoura et al.(2013), Noguchi (2018), Yang and Yuan (2019) and references wherein.

The idea to consider the mixture of both Nash and cooperative equilibria together was originally studied by Zhao (1992) under the name called "Hybrid Solution". Building off Zhao (1992) and Kajii (1992), and supported by recently work under Yang and Yuan (2019), we are able to establish a new tool by "Consensus Games" in topological vector spaces without ordered preferences from the viewpoint of Blockchain in Fintech.

Briefly, the “Consensus Game” is a new concept which allows us to discuss if there exists an acceptable (maybe not “Pareto optimal”) collaborative strategy which consists of cooperative and non-cooperative behaviors together under a given consensus principle such as to apply “Longest Chain Rules (LCR)” due to Nakamoto (2008) consensus. Briefly, we define a miner acting by a cooperative strategy behavior under the framework of mining Bitcoin if the miner applying the general principle of Nakamoto’s consensus protocol, in particular applying at leat (LCR); otherwise, the miner is said to play in mining-pool games in non-cooperative strategies, for this situation, one of the typical behaviors is that a miner mines for Bitcoin by acting as a “selfish miner” or “mining-pool attacker” for the purpose to violate the LCR for a high reward block and associated activity against the general principle of a given “consensus” (see more for related related materials and disucssion given by Nyumbayire (2017), Biais et al.(2019) and reference wherein for the discussion with or without occurring forks for blockchain acting as a platform called the “Blockchain Ecosystems” or “Consensus Economics”). Thus, when comparing with the traditional cooperative and non-cooperative game, the consensus game is a natural extension for a consensus economy, especially under the framework of the Bitcoin ecosystem associated with Nakamoto’s consensus protocol. We note that mining pool games were extensively studied by Kroll et al. (2013), Eyal et al.(2014), Eyal (2015), Bonneau et al. (2015) (see also Carlsten et al. (2016), Kiayias et al.(2016), Sapirstein et al.(2016) and references wherein), smart contracts were discussed by Cong and He (2019), and finally move toward blockchain-based accounting and assurance given by Dai and Vasarhelyi (2017) and many others. But one critical issue still remaining is: “*if it is possible to have a general consensus to lead the Mining-Pool Game stable (see the meaning in details below) in supporting the Blockchain ecosystem running?*”

Based on the meaning for consensus games above (see also Section 2 below), it seems that the notion of consensus equilibria for consensus games with a partition of the set of players through the general profit functions as payoff functions (which are nonordered preferences mappings) in game theory and related forms would be a useful tool for the study of consensus economics under the framework of Blockchain as a new tool, our goal in this paper is to discuss one of the most fundamental questions for consensus economics in Fintech as follows:

“ Is it possible to have a general consensus (for example, the Nakamoto’s one) to lead the Mining-Pool Game stable in supporting the Blockchain ecosystem to run (even with existing attacker) in the sense that

(1) there always exists honest miners maintaining the Mining Longest Chain Rules

(LCR) (given the plausibility of mining-pool attacking); and

(2) Bitcoin ecosystem always works (or, majorities of miners do not collude to break it; here the term "collusion" means an attempt to violate the LCR and for a high reward block, see the discussion on this issue by Saleh (2020))?"

The work of this paper is as follows: We first discuss a new concept called "Consensus Game" (CG) with motivation from the mechanism design for the blockchain in financial technology under the consensus incentives introduced by Nakamoto (2008) (see also Biais et al.(2019), Cong and He (2019), Narayanan et al.(2016), Nyumbayire (2017) and related references wherein). Starting from results by Zhao (1992) to Yang and Yuan (2019) where a number of existence results have been established for a general game, while our paper mainly captures the consensus idea of blockchain consensus in Fintech, and the work of Yang and Yuan (2019) plays an important role in modelling the Blockchain in Fintech. After we give an outline how the general existence results of consensus equilibria for consensus games is formulated as the existence for the general stability of Mining Pool Games, we then establish general existence results for the consensus equilibria of general gap games for miners by using miners' profit functions directly as payoff ones in game theory, which not only help us to claim the existence for the general stability for Gap games under the general framework of Blockchain ecosystems, but also allow us to illustrate a number of different phenomenons on the study of mining pool-games with possible impacts due to Mining Gap Games behaviors with scenarios embedded in Bitcoin economics.

Here we like to point out that (see also Tsbary and Eyal (2018)) that the a Mining Gap Behavior Game is indeed the game (of mining Bitcoin) played among all miners, which is a one-short game on finding blocks: The first to find a block gets rewards, while all suffer expenses. Thus all miners decide when to start their mining rigs, and strive to optimize their average revenue, maximizing the difference between their income and expense. The one situation for Gap Game is that for miners under the framework of general incentives consensus in which miners would "avoid mining blocks" when the available fees are insufficient (this situation is called a Gap behavior for a miner in mining-pool games. In particular, if incentives come only from fees, then a mining gap behavior would happen, and may impact the stability of bitcoin (as without the block reward, see more in details with discussion given by Carlesten et al.(2016) and references wherein), we will show how this problem can be done by using payoff functions under the framework of consensus games in Sections 3 and 4 below.

We also like to share with readers that in this paper, the way we give an outline how the stability (in terms of the existence of equilibria) for ming pool-games can be formulated as an application of consensus games by using the concept of consensus equilibria, could be used as a fundamental tool for the study of consensus economics under general framework of Blockchain economy in Fintech.

The rest of this paper is organized as follows. Section 1 is an introduction, Section 2 gives the general existence results for consensus games which will be used as a tool used in Section 4. In Section 3, we discuss the consensus equilibria for mining-pool games and then related to the stability related to mining Gap games behaviors under the environment for Blockchin ecosystems. Then in section 4, our job is to establish the general existence results of consensus equilibria for Gap games in general, and then to answer the stability problems of Blockchain Ecosystems mentioned above affirmatively under the possible environment of miners' Gap behaviors in mining bicoin economics. As applications, we will illustrate a number of different phenomenons on the study of mining pool-games with possible impacts due to miners' gap behaviors with scenarios embedded in Bitcoin economics. Our study on the explanation for the stability of mining gap game for Blockchain ecosystems shows that the concept of consensus equilibria may play a important role for the development of fundamental theory for consensus economics. Section 5 is with the conclusion.

2 The Concept of Consensus Games

In this section, based on hybrid solutions in game theory, we fist introduce a new concept called "Consensus Game" (in short, "CG"), which will be used in consensus economics to describe what kinds of general consensus (through the realization of mechanism design) will achieve incentive compatibility to fight against the non-cooperative behaviors (i.e., refusing following "Nakamoto's consensus", but taking such as "selfish mining" or "mining pool with attacking" strategy) for the coalition of participants (agents) under the platform of Blockchain. Then we will discuss the existence of general consensus games' equilibria by using the concept of hybrid solutions. For the related reference on Blockchain and related Nakamoto consensus Nakamoto (2008), see Kroll et al.(2013), Eyal and Sirer (2014), Eyal (2015), Bonneau et al.(2015) (see also Carlsten et al.(2016)), Kiayias et al.(2016), Sapirstein et al. (2016), Biais et al. (2019), Nyumbayire (2017), Narayanan et al.(2016)) and related references wherein.

We know that under the Nakamoto consensus protocol introduced in Year 2008, one key issue is to find a set of rules (for consensus) to encourage agents (miners from mining pools) to follow rules truthfully under the corresponding (consensus) protocol which may be formulated as preference mappings under the framework of abstract economy models (see Yannelis and Prabhakar (1983), Yuan (1999) and references wherein), thus it is very important to study the stability of Blockchain consensus in terms of the existence for equilibria of miners (from mining pools) to follow the so-called "LCR" (also see the discussion in Section 3 below) while with or without occurring of forks for blockchain of Bitcoin ecosystems. Of course, some other issues needed to be considered are possible collusive equilibria (see Saleh (2020) and reference wherein) and their behavior related to smart contracts, or dynamic equilibria under blockchain disruption as initially discussed by Cong and He (2019), and other issues such as emerging blockchain-based accounting and assurance outlined by Dai and Vasarhelyi (2017), discussed by Narayanan et al.(2016), and also see Saleh (2020) and references wherein for the study of these questions.

Using the framework of the blockchain and associated consensus mechanism, the stability (in terms of existence for equilibria)for the mining pool game can be formulated as the problem to find a strategy under which some group of miners (called, "honest miners") in the mining-pools (for Bitcoins) to follow up "LCR behaviors" respect to either noncooperative or cooperative behaviors though maybe some miners may take "selfish mining" or " mining pool with attacking" strategies, this situation by the mixing of both cooperative and non-cooperative game behaviors is exactly the notion for the concept of "hybrid solution" for games given by Zhao (1992), we thus come to have the following definition for a Consensus Game (in short, "CG") as follows:

Given a consensus $\mathbf{G}$ (by consisting of a number of rules), let $N = \{1, 2, \cdots, n_0\}$ be the set of agents and $p = \{N_1, \cdots, N_{k_0}\}$ be a partition of N (as defined above), and $\mathcal{N}$ is all subsets of N. For each $i \in N$, the mapping $u_i : X \longrightarrow R$ is the payoff function of player i determined by the rules of the consensus $\mathbf{G}$, we say that a normal form of consensus game (CG) is just the following form:

$$CG := (\mathbf{G}, N, p, (X_i, u_i)_{i \in N})$$

We say the consensus game CG has a consensus equilibrium if the corresponding formal form of the game $(N, p, (X_i, u_i)_{i \in N})$ has a hybrid solution (see Zhao (1992) for the definition, see also Di et al.(2019)). Basically, the hybrid solution for the finest partition (i.e., $k_0 = n_0$, and the partition $P = N$) is a Nash equilibrium; and in general the hybrid solution is the α-core for the coarest paetition that consists of the grand coalition alone. The hybrid solutions are more general because of the coexistence of competition and cooperation, which captures the ommipresent situation in which a group (pool) of miners behave collectively to complete with other groups (pools) of miners.

Throughout the rest part of this paper, when mentioning the consensus game (CG), we always assume it associated with the consensus **G** and omit it if no confusion. We now have the defining consensus equilibria for the consensus games with nonordered preferences.

A consensus game can be defined by

$$CG = (N, p, (X(t))_{t \in N}, P),$$

where $p = \{N_r | r \in R\}$ is a partition of N, which is a set of all miners in mining-pools for mining Bitcoin, $X(t)$ is the strategy space (sets) of miner or saying, the player t's all mining strategies (behaviors), and $X = \prod_{t \in N} X(t), X(S) = \prod_{t \in S} X(t), X(-S) = \prod_{t \notin S} X(t), \forall S \in \mathcal{N}$, $P(t, \cdot) : X \rightrightarrows X$ is the preference mapping of player t under a given consensus (e.j., the Nakamoto (2008) consensus protocol). A point $x^* \in X$ is a consensus equilibrium of CG if for any $N_r \in p$ and any $S \in \mathcal{N}_r$, there exists no $y(S) \in X(S)$ such that

$$\{y(S)\} \times X(N_r - S) \times \{x^*(-N_r)\} \subset P(t, x^*), \ \forall t \in S.$$

Briefly to say, the above express means that there is no any other better Parteto optimal solution than x^* if considering both cooperative and non-cooperative strategies together in mining for Bitcoins of mining-pool games.

We now list the following result which will be used as a tool to discuss the stability of Ming Gap Games under the framework of Blockchain Ecosystems (which is the Corollary A.1 given by Appendix A).

Theorem 2.1 *Suppose that a normal-form game with a partition*

$$G = (N, p, (X_i, u_i)_{i \in N})$$

satisfies the following conditions:

(i) N is a finite set;

(ii) for each $i \in N$, X_i is a nonempty convex compact subset of a Hausdorff topological vector space E_i;

(iii) for each $i \in N$, u_i is continuous and quasiconcave on X.

Then there exists at least a hybrid solution of G (thus the consensus equilibrium of consensus game G).

In this section, the consensus games' results are mainly based on the existence results of theoretical models in game theory first established by Yang and Yuan (2019) (see also Di et al.(2019)).

The Theorem 2.1 above will be used as a tool in Section 4 below to discuss the general stability problems of mining pool-games for miners under the framework of Blockchain consensus, which will be used to illustrate a number of scenarios embedded by miners' gap behaviors for consensus economics.

3 The Consensus Equilibria of Mining Gap Games and Applications

In this section, we first discuss the general stability problems related the study from a number of literatures for mining pool-games of Bitcoins consensus principle due to Nakamoto introduced in 2008's, and then we establish the general existence results for consensus equilibria of mining-pool games. As applications, our discussion with illustrations for some issues and questions from mining pool games shows that the concept of the consensus games would play a key role for the study of consensus economics in Fintech.

In general, Bitcoin's blockchain protocol provides two incentives for miners: "*Block rewards*" and "*transaction fees*," which are key drivers for Bitcoin ecosystems. The former accounts for the vast majority of miner revenues at the beginning of the system, but it is expected to transition to the latter as the block rewards dwindle. There has been an implicit belief that whether miners are paid by block rewards or transaction fees does not affect the security of the block chain. But Carlsten et al. (2016) (see also Kroll et al. (2013), Eyal and Sirer (2014), Eyal (2015), Bonneau et al. (2015) and a number of related references wherein) show that this is not the case, their key insight is that with only transaction fees, the variance of the block reward is very high due to the exponentially distributed block arrival time, and it becomes attractive to fork a "*wealthy*" block to "*steal*" the rewards therein. They show that this results in an equilibrium with undesirable properties for Bitcoin′s security and performance, and even non-equilibria in some circumstances. Moreover, they also study selfish mining (see Eyal and Sirer (2014)) and show that it can be profitable for a miner with an arbitrarily low hash power share, who is arbitrarily poorly connected within the network, or working by themselves (i.e., miners' behavior in noncooperation games' way). Thus we need to consider the stability of Bitcoin ecosystems in the sense that if there is the existence of a hybrid solution (thus, the consensus equilibrium as introduced in this paper) for a mining-pool games with honest and dishonest miners to mine together with mixture by following either cooperation or non-cooperation game's behavior, in particular, for the miners' working behavior and strategy (also called "*mining for Bitcoin*") in different pools for the implementation of the most important parts due to Nakamoto's consensus being so-called the "*proof of work*" mechanism in Bitcoin economics.

In particular, we will focus on the general discussion for the mechanism of the phenomenon called " Mining Gap Behavior " (in short, "Gap Games") for miners under the framework of general incentives consensus in which miners would avoid mining blocks when the available fees are insufficient, in particular, if incentives come only from fees, then a mining gap behavior would happen, for more in details, see Carlesten et al.(2016) and related references wherein. Based on our results, we are able to answer one of the most fundamental questions in consensus economics in terms of consensus games affirmatively as follows (as the question raised in Section 1):

"Can we always design a reasonable consensus (for example, due to Nakamoto Consensus given in Year 2008) to lead the mining-pool game stable (even with the behavior of miner's gap game behaviors existing) in the sense of the existence for consensus equilibria under the framework of the Blockchain ecosystem respect to following two respects:

(1): there always exists honest miners keeping "Mining Longest Chain Rules (LCR)" (though maybe with or without either "Occurring Gap Behavior, or Fork Chain" for blockchains), plus the plausibility of mining-pool attacking; and

(2): Bitcoin ecosystem always works (as the majorities of miners do not collude to break it; here the term "collusion" mainly means an attempt to violate the LCR and fork a high-reward block;see Saleh (2020) for the discussion in details on this problem)? "

Furthermore, our applications with illustrations by discussing some issues and problems on the stability of mining pool-games for miners by using consensus games show that the concept of consensus equilibria could be used as a fundamental tool for the study of consensus economics under the framework of Blockchain economy in Fintech.

3.1 The Meaning of the Stability for Bitcoin Ecosystems

We know that Bitcoin is the first widely popular cryptocurrency with a broad user base and a rich ecosystem, all hinging on the incentives in place to maintain the critical Bitcoin blockchain. For blockchain which acts as a platform (or saying, a new kind of data structures, or a tool) in supporting businesses under the Bitcoin ecosystem, a natural process leads participants of such systems to form pools where members aggregate their power and share the rewards. Experience with Bitcoin shows that the largest pools are often open, allowing anyone to join. On the other hand, it has long been known that a member can sabotage an open pool by joining but never sharing proofs of work (this miner is also called "attacker") . The pool shares its revenue with the attacker, and each of its participants earns less (see the discussion by Kroll et al.(2013), Eyal et al.(2014), Eyal (2015), Bonneau et al.(2015), and also Carlsten et al.(2016), Kiayias et al.(2016), Sapirstein et al. (2016), Tsabary and Eyal (2018) and references wherein).

Thus open pools are susceptible to the classical block withholding attack (e.g., see Rosenfeld (2011), and Kroll et al. (2013), Eyal et al.(2014), Eyal (2015), Bonneau et al. (2015)), where a miner sends only partial proof of work to the pool manager and discards full proof of work. Due to the partial proof of work sent to the pool by the miner, the miner is considered a regular pool member and the pool can estimate its power. Therefore, the attacker shares the revenue obtained by the other pool members, but does not contribute. It reduces the revenue of the other members, but also its own.

Moreover, by following Bonneau et al.(2015), in general we face two opposing viewpoints on Bitcoin in straw-man form: The first is that "*Bitcoin works in practice, but not in theory*"; A second viewpoint is that "*Bitcoin′s stability relies on an unknown combination of socioeconomic factors which is hopelessly intractable to model with sufficient precision, failing to yield a convincing argument for the system′s soundness*".

By putting above two opposing viewpoints on Bitcoin together, and incorporating Bitcoin's three main (technical) components: "*Transactions (including scripts)*," "*Consensus protocol*," and "*Communication network*" as a whole, we do think it is critical to study the so-called "Stability" (with more explanation below) for Bitcoin respect to its three main components in terms of a complex ecosystem.

For the comprehensive study on the explanation for the different aspects of the meaning on the stability for mining-pool games, we refer to Bonneau et al.(2015) and references wherein, here once again the meaning for the stability we only focus as the following question in terms of existence for equilibria for miners mining bitcoin in mining pool games:

"Is if there the existence of a consensus (hybrid solution) (thus, the consensus equilibrium as introduced in this paper) for a mining-pool games with honest and dishonest miners with mixture of either cooperative game or non-cooperative game's behaviors, in particular, for the miners' working behavior and strategy in different pools for the implementation of the most important parts due to Nakamoto's consensus being so-called the "Proof of Work" mechanism in Bitcoin economics?"

There are many discussion on the explanation for the possible meaning on the stability, see Bonneau et al.(2015), Garay et al.(2014), Kroll et al.(2013), Miller and La Viola Jr (2014) and references wherein, but here we list two aspects below related to the meaning of the stability in general.

1) The stability with bitcoin-denominated utility: We may ask *if simple majority compliance may not ensure fairness?* By an interesting non-compliant mining strategy which is temporary block withholding as discussed by Bahackm (2013), Eyal and Sirer (2014), Garay et al.(2014) and others; we may also ask *if majority compliance is an equilibrium with perfect information* as shown by Kroll et al.(2013); and also can ask *if majority compliance may imply convergence and consensus* as discussed by Miller and La Viola Jr (2014) and Garay et al.(2014).

Secondly, one of the most important situations is that *with a majority miner, if stability is not guaranteed?* We like to mention that for the stability in terms of issue "*if mining longest chain rules*" (LCR) was also discussed by Biais et al.(2019) through the Markov chain method under the situation with, or without mining a fork at the same time (i.e., the weak stability). Thus it is very important to discuss if it is possible among miners (in terms of either coordination (cooperation) or noncooperation behavior) for Bitcoin blockchain on mining LCR (while, with, or without occurring forking) as indeed a fork can also occur even when some miners adopt a new version of the mining software that is incompatible with the current version (if miners fail to coordinate on the same software, this triggers a fork).

Furthermore, in line with Nakamoto (2008), it is said that the Bitcoin blockchain protocols are prone to multiple equilibria with forks due to the strategic complementarities of miner's actions, is it true? We would ask, *is the stability there if miners collude?*(see the study by Saleh (2020)); and the question: *is stability there if mining rewards decline?* In particular, for the following issue:

2) The stability with incentives other than mining income: At least two strategies have been analyzed which may be advantageous for a miner whose utility is not purely derived from mining rewards, they are *Goldfinger attacks* (see also Kroll et al.(2013)), and *Feather-forking* proposed by Miller (2013).

Thus one of the key issues for mining pool needs is to consider is *what could go wrong* for the situation called "*Mining Gap*" which means if without a block reward immediately after a block is found if there is zero expected reward for mining but nonzero electricity cost, then it would be unprofitable for any miner to mine? (see, Bahackm (2013), Eyal and Sirer (2014), Tsabary and Eyal (2018) and related literature wherein).

In what follows, we will discuss how to establish an outline how to explain the stability of Bitcoin system as the existence of consensus equilibria under the framework of consensus games with focus on the consensus associated with Bitcoin ecosystem. We now first give a brief recalling for the description of basic mining economics associated with "**three types of consensuses**" in general below.

3.2 The Explanation of the Stability for Mining Pool Games by the Concept of Consensus Games

Success of the Bitcoin economy requires that Bitcoin's distributed protocols operate and remain stable, which relies on "**three types of consensuses**" at least:

1 Consensus about Rules: Players must agree on criteria to determine which transactions are valid. Only valid transactions will be memorialized in the Bitcoin log, but this requires agreement on how to determine validity.

2 Consensus about State: Players must agree on which transactions have actually occurred, that is, they must agree on the history of the Bitcoin economy, so that there is a common understanding of who owns which coin at any given time.

3 Consensus that Bitcoins are Valuable: Players must agree that Bitcoins have value so that players will be willing to accept Bitcoins in payment.

Each of these forms of consensus depends mutually on the other two. For example, it is hard to agree on the history without agreeing on the rules, and it is hard to believe in the value of a Bitcoin if participants cannot even agree on who owns which Bitcoin. Consensus about state is a technological problem in distributed systems design. Each player can see part of the state and the players need to cooperate, in large numbers and across a potentially unreliable network, to achieve a consistent understanding of the global state. Technological consensus must be achieved despite the possibility that some players will deviate from the published rules. In the distributed systems literature, devious behavior ("Byzantine failures") can often be tolerated if a sufficient majority of players are honest and cooperate. However, in Bitcoin, we explicitly assume that players will behave according to their incentives (assuming cooperation despite incentives to the contrary would make the design much simpler, though unrealistic.)

Game-theoretic issues are very important for the correct execution of the blockchain protocol. This was realized at its inception when its creator, Nakamoto (2008) analyzed incentives in a simple, albeit insufficient, model. Understanding these issues is essential for the survival of bitcoin and the development of the blockchain protocol. In practice it can help understand their strengths and vulnerabilities and, in economic and algorithmic theory, it can provide an excellent example for studying how two rational ("*selfish miners*") players can play games in a distributed way and map out their possibilities and difficulties (e.g., see the Miners Dilemma discussed by Eyal (2015) as one example).

Distilling the essential game-theoretic properties of blockchain maintenance is far from trivial; some "*attacks*" and vulnerabilities have been proposed but there seems to exist no systematic way to discover them. In this paper, we will study two models' situations of mining pool-games as applications of our consensus games below in which the miners (the nodes of the distributed network that run the protocol and are paid for it) play a complete-information. We also mention that the case of incomplete-information situations which may or may not be under the framework of stochastic games, is not our focus here, as one of our focus in this paper is to show how the concept of consensus game useful for the study of mining pool games, in particular for mining gap games.

Meanwhile, a number of works have focused on a rational analysis of the system (see Rosenfeld (2011), Carlsten et al.(2016), Eyal and Sirer (2014) and references wherein). Take a long story as a short one, these works treat Bitcoin as a game between the (competing) rational miners, trying to maximize a set of utilities that are postulated as a natural incentive structure for the system. The goal of such an analysis is to investigate whether or not, or under which assumptions on the incentives and/or the level of collaboration of the parties, Bitcoin achieves a stable state, i.e., a game-theoretic equilibrium.

As discussed briefly above, we may interpret the behavior of "attackers" as miners playing noncooperative games by taking different kinds of attack strategies, and "honest miners " playing cooperative games by following the "default compliant mining rule" of Bitcoin consensus in applying LCR. The existence of the Bitcoin ecosystem's stability is equivalent to the existence of (hybrid) equilibrium which is the so-called "consensus equilibrium" of the "consensus game" defined above in this paper.

Therefore the existence of consensus equilibrium for consensus games under the general framework of Bitcoin consensus means there always exists a group of people working on the "Longest Chain Rule" (LCR) which assures the Blockchain under the Bitcoin consensus is properly maintained (though some miners working on forks, other miners do not, e.g., see also Biais et al.(2019) in addressing this issue in terms of Markov perfect equilibrium). Thus the study for the existence of consensus equilibrium for consensus games provide the fundamental base for consensus economics in general. In this way, we can establish the stability of mining games for Bitcoin as applications of the general existence results established for consensus games above in this paper as shown below by Theorems 3.1 to 3.3, and Remarks 3.1 to 3.4).

3.3 The Framework of Mining Gap Games and related Stability

Blockchain-based cryptocurrencies secure a decentralized consensus protocol by incentives. The protocol participants, called "Miners" (also called, "Player", or "Controller") generate (mine) a series of blocks, each containing monetary transactions created by system users. As incentive for participation, miners receive newly minted currency and transaction fees paid by transaction creators. Blockchain bandwidth limits lead users to pay increasing fees in order to prioritize their transactions. However, like Tsabary and Eyal (2018) point out that by so far the most work focused on models where fees are negligible except that Carlsten et al.(2016) discussed that if incentives come only from fees then a mining gap would form: The miners would avoid mining when the available fees are insufficient.

In this part, it is our goal to establish general existence results for the consensus equilibria of general Gap Games by using corresponding payoff functions (for profit functions) directly, which then used to illustrate some specifical issues and problems on the stability of mining pool-games with different behaviors by miners, and then using results to explain the possible scenarios for different situations of Blockchain Ecosystems as did by Tsabary and Eyal (2018) (they use the concept of utility function). Our study on the stability of Gap Games for Mining Pools by applying consensus games shows that the concept of consensus equilibria would play a key role for the explanation of different scenarios from consensus economics in general.

3.3.1 The General Framework of Mining-Pool Games

In the mining-pool games, we consider the model which is a system with a fixed set of miners and a fixed set of mining rigs and each miner controls at least one rig and each rig is controlled by exactly one miner under the general framework by assuming the homogeneity of cost structure and with symmetry of information for all miners. Second, we assume for simplicity that mining rigs are identical (as did by Carlsten et al.(2016)). Third, we assume that rigs have two states:

1) “ off state” as the default state; and

2) “on state” (which means it keeps running until finding a valid block).

Each miner assigns a start time for each of her controlled rigs, in which the rig is turned on, and we also often refer to a turned-on rig as an “active rig”.

Once a rig is turned on, the time it takes to find a valid block is exponentially distributed with a fixed rate parameter, which is shared among all rigs (see Eyal and Sirer (2014), Nayak et al.(2015), Sapirstein et al.(2016) and references wherein). Therefore the time to find the first block by any of the rigs is the minimum of all finding times by all different rigs. The value of the rate parameter is determined by the cryptocurrency protocol such that the expected block time interval is of a constant value that is also determined by the protocol. The rate parameter represents the difficulty of the cryptographic puzzle, and we use the terms difficulty and rate interchangeably. The assigned start times of rigs by miners affect the value of the rate parameter. If blocks are found too fast (too slow), then the difficulty parameter value is changed by the protocol to decrease (increase) the rate of each individual rig. In equilibrium, the rate parameter is of a fixed value.

The rig that finds the block first awards its controlling miner the block reward, which is comprised of two parts. The first part is fees reward that comes from aggregation of newly introduced transactions to the system. This reward is time-dependent, as the time progresses there are more pending transactions in the system, and the potential fees reward grows. The second part is a subsidy we refer to as base reward, which to the contrary of the fees reward is fixed over time. This reward is comprised of the minting of new currency with the creation of each block, as well as the expected reward from transaction fees considering the expected initial set of pending transactions. Note that the finding of a new block does not reward any other miners except the miner who found it.

To participate in the system miners expend resources, and we differentiate two types of such resources. First, miners have capital expenses (denoted by "Capex"), which are for owning a rig (see Digiconomist.net (2017), Twiner (2017)) and apply whether the rig is active or not. Miners also have operational expenses (denoted by "Opex"), which are paid for having a rig actively mining (see Digiconomist.net (2018a) and Digiconomist.net (2018b)), i.e., owning an active rig. Note that these expenses apply for all miners and not just on those who manage to successfully mine blocks.

Once a block is found, all miners move on to find the next block. This process is repeated indefinitely. The profit of a miner for each block is the difference between her total expenses and her total reward. Rational miners strive to maximize their profits, giving rise to a game. But now, the most fundamental question is the following one:

"Do we have a class of honest miners to maintain Bitcoin ecosystems by applying Mining Longest Chain Rules (in terms of Pareto optimal strategies to maximizing their profits under the framework of mining Gap Games behaviors)?"

In what follows, we go to establish the general existence for consensus equilibria of mining-pool games which indeed answers above question positively, and thus confirming the existence for the stability of mining gap games which is one of the most fundamental questions for consensus economics affirmatively as raised in Section 1.

3.3.2 The Concept of General Gap Games for Miners

We know that the behavior of mining-pool games play a critical role for the Blockchain ecosystems in general by a simple fact that Blockchain based cryptocurrencies secure a decentralized consensus protocol by incentives. The protocol participants, i.e., miners generate (mine) a series of blocks, each containing monetary transactions created by system users. As incentive for participation, miners receive newly minted currency and transaction fees paid by transaction creators. Blockchain bandwidth limits lead users to pay increasing fees in order to prioritize their transactions. However, we must face one fundamental question is (e.g., see Carlsten et al.(2016)) if incentives come only from fees, then a mining gap may happen in the sense that "miners would avoid mining when the available fees are insufficient" in the practice, for the related information, related background and discussion, see Carlsten et al.(2016), Eyal and Sirer (2014), Tsabary and Eyal (2018) and references wherein.

By following Tsabary and Eyal (2018), the repeated search for the blocks becomes a series of independent one-shot competitions, in each only one miner gets the reward but all miners pay expenses. To reason about expected revenues, rather than considering the individual iterations we consider a one-shot game played by the miners. A player's strategy is the choice of start times of all of her rigs: when each rig is turned on. The choice of start times are made a-priori by all players. We define the profit (but the corresponding utility of a player to be her/his expected profit), which is her/his expected income minus her/his expected expenses at a given time t.

We recalled that a "Gap Game (GP)" indeed is a set of miners $N := \{1, 2, \cdots, n\}$ with a partition $N_1, N_2, \cdots, N_k$ of N which is a system (consisting of n mining rigs controlled by k players), each N_j is a player, where $j \in K = \{1, 2, \cdots, k\}$: The player j controls the set of rigs with indices R_j. Note that for any $j, i = 1, 2, \cdots, k$, where $i \neq j$, we have $R_j \neq \emptyset$, $R_i \cap R_j = \emptyset$ and $N = \cup_{i=1}^{k} R_i = \{1, 2, \cdots, n\}$.

Denote the expected block time interval achieved by the protocol by "Block-Interval". The start time of each rig j is s_j, and we denote the normalized start time by $\hat{s}_j := \frac{s_j}{Block-Interval}$.

Once a rig is turned on, we assume that the time the rig requires to find a block follows "an independent exponentially distributed with a rate parameter $\mu(\hat{s})$)".

For the convenience, we denote $\hat{s}$ as the vector of increasing order n rigs' start times. We also assume that all rigs are identical (i.e., with the computing power). Each mining rig costs "C_{cap}" per time unit for the ownership explained as the capital cost (for example), and "C_{op}" per time unit if it is turned on explained as operation cost.

We note that the strategy space does not include turning rigs off, as this is an irrational behavior. Block finding time of an active rig is drawn from the exponential distribution, which is memoryless. That means the probability for a rig to find the block in some time interval is not affected by how much time had already passed since that rig began mining. Therefore, a single rig′s chances of finding a block are not decreasing over time. Recall that the total reward also increase over time. Hence, if at some point in time the reward justified turning a rig on, then this justification holds from that time until the block is found.

3.3.3 The Framework of Fees Reward Accumulation and Related Costs

We all know that the costs of mining-pools' parameters values are affected by a wide range of factors, stemming from different sources. The fees are affected by the system users and the market (see Binns (2018), Blochchain.info (2018a, 2018b, 2018c), Earn.com (2018), Khatwani (2018) and Moser and Bohme (2015)). The base reward is also affected by systems user and market, as these affect the residual fees, but also by the minting rate, which is defined by the cryptocurrency protocol. The capital cost (denoted by "Capex") is affected by factors such as technological advancements of mining rigs efficiency (see Biais et al. (2019)), personnel wages, and real estate costs (see Digiconomist.net (2017), Malkin (2018), Wang (2017) and references wherein). The Operational cost (denoted by "Opex") is affected primarily by the electricity costs (see Browne (2017), Digiconomist.net (2017, 2018a, 2018b)) for operating the mining rigs. That includes both the actual puzzle solving process as well as cooling expenses. These parameters are therefore not only difficult to estimate, but they vary between different currencies, and also over time for the same currency. Hence, we analyze the system for a range of parameters values to make general observations, focusing on trends that are robust across the parameter range. We begin by analyzing how fees accumulate in the system, and then move towards determining parameter values which we will be used throughout the rest of this work.

Based on the study of Tsabary and Eyal (2018) on the fees reward accumulation over time, without loss of the generality, it seems reasonable to used the linear regression to measure the fee reward accumulation over time. Hence, we may model the total block reward as a linear function, where the slope is the expected fees accumulation rate, and the intercept is the sum of the newly minted currency and the expected feesavailableimmediatelyafterablockisfound.Werepeatedthese measurements at other dates for different periods of time and received similar results. We denote λ_t as the "**fees accumulation rate**" and λ_0 as the "**base reward**". In order to see how important among λ_0 and λ_t, we have the following notation:

We denote by “Expected-Total-Fees” the expected total fees accumulating during the expected time to find a block, namely,

$$\text{Expected-Total-Fees} := \text{Block-Interval} \cdot \lambda_t,$$

and define

$$\text{EBRR} := \frac{\lambda_0}{\text{Expected-Total-Fees}}.$$

By the fact that we assume any miner has only one option either joining or leaving the system, and for the simplicity, we may suppose the cost of C_{op} and C_{cap} are a fixed amount.

Next we need to build the profit function $P_i(t)$ for each $i = 1, 2, \cdots, k$ at time t, which allow us to establish the general existence of consensus equilibria for Gap Games described in this section.

3.3.4 The Profit Function of Mining Gap Games

In order to find the profit (and associated utility) function for each player i of Gap Games at time t, we start by analyzing the block finding time's probability distribution, this is a payoff function of the players$'$ selection for the start times. We model the block finding time as a random variable denoted by B with cumulative distribution function (CDF) denoted by $F_B(t; \hat{s}, \mu(\hat{s}))$, and probability density function (PDF) denoted by $f_B(t; \hat{s}, \mu(\hat{s}))$ (explained below), respectively.

Then a given miner $i = 1, 2, \cdots, k$, assume a single rig $j \in R_i$ with start time s_j. We denote the time this rig requires for finding a block as a random variable B_j. Recall that the rate of a single rig is $\mu(\hat{s})$, which is set by the protocol. The value of B_j is drawn from the shifted exponential distribution, with a shift of s_i and rate $\mu(\hat{(s)})$.

By the fact that all rigs are competing on finding the next block, the rig that finds the next block first is the rig with the minimal value of B_j, thus the time required for finding the next block is given by the following stop time process B defined as a stop time process:

$$B := \min_{j \in \{1,2,\cdots,k\}} B_j.$$

For any time t and any player i, the active set $\text{active}_i(t)$ is defined as

$$\text{active}_i(t) := \{j \in R_i : s_j \leq t\}$$

and we also define

$$\text{active}(t) := \cup_{i=1}^{k} R_i.$$

Then the corresponding CDF is given by (see details given by Appendix B):

$$F_B(t; \hat{s}, \mu(\hat{s})) = 1 - Pr(t \leq B) = 1 - \exp(-\mu(\hat{s}) \cdot \Sigma_{j \in \text{active}(t)}(t - s_j)),$$

and corresponding PDF is given by

$$f_B(t; \hat{s}, \mu(\hat{s}))) = \mu(\hat{s})) \cdot |\text{active}(t)| \exp(-\mu(\hat{s})) \cdot \Sigma_{j \in \text{active}(t)}(t - s_j)),$$

where $|active(t)|$ denotes the absolute value of $active(t)$.

Recall that once a rig is turned on, the time it requires to find a block is drawn from the exponential distribution. The exponential distribution is memoryless, meaning the time that passed does not affect the chances of a rig to find the block. Since the rate parameter $\mu(\hat{s})$ is shared among all rigs, at any given time all the active rigs have the same chance to find the block, regardless of how much time they had been active for already. By the fact that the set of active rigs at the time the block is found active(t), the probability of a specific active rig to find the block is one divided by the total number of active rigs. Note that since the block was found at time t, then there exists $j \in \{1, 2, \cdots, k\}$ such that $s_j \leq t$ and thus $|\text{active}(t)| > 0$. As Players may control many rigs, so the probability that player i controls the rig that found the block is he number of her controlled active rigs divided by the total number of active rigs. We denote the ratio of player i's active rigs out of all the active rigs at time t by $\alpha_i(t)$ at time t defined by

$$\alpha_i(t) := \frac{|\text{active}_i(t)|}{|\text{active}(t)|}.$$

It is clear that the ratio $\alpha_i(t)$ is continuous in t, and is also the expected factor of player i's portion of the total reward. Thus for a block is found at time t, the expected income (denoted by $\text{E}(\text{Income}_i|B = t)$) of player i at time t is

$$\text{E}(\text{Income}_i|B = t) = \alpha_i(t) \cdot (\lambda_0 + \lambda_t \cdot t).$$

We also recall that players in general have two kind of expenses (see also Tsabary and Eyal (2018)): The first one may be called "Capex", would be explained for the capital cost such as for "owning a rig"; and the second one called "Open", for example, which would be explained for the operation cost such as for "keeping a rig active". As Capex applies for all rigs controlled by the player, whether they are turned on or not, it follows for each rig, the capex it imposes by time t is the $C_{\text{cap}} \cdot t$.

On the other hand, recall that R_j is the set of rig indices that player j controls, which totals with $|R_j|$ rigs, thus the total Capex of player j at time t are $C_{\text{cap}} \cdot |R_j| \cdot t$.

Considering the Opex applies only for active rigs, for each active rig, the expenses it imposes by time t is the product of C_{op} and the time duration this rig is turned on already: At time t, the active rig j with s_j has been active for the time of $t - s_j$. Then the expected expenses (denoted by $E(\text{Expense}_i|B = t)$) of player i at time t is given by

$$E(\text{Expense}_i|B = t) := C_{\text{cap}} \cdot |R_i| \cot t + C_{\text{op}} \cdot \Sigma_{j \in \text{active}_i(t)}(t - s_j).$$

Now for a given miner (player, or saying, controller) i at time t, we can define its Profit Function P_i through the expected income function and expense function as given below:

$$P_i(t) := E(\text{profit}_i|B = t) = E(\text{Income}_i|B = t) - E(\text{Expensive}_i|B = t)$$

where $E(\text{Income}_i|B = t)$ and $E(\text{Expensive}_i|B = t)$ are expected income and expenses at time t for a given Gap Game. As discussed above, we assume its reward function is given by the following form:

$$E(\text{Income}_i|B = t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t)$$

We also mention that for more general study on the reward function with incentive compatibility for Bitcoin mining pool, the interested readers are referred to Schrijvers et al.(2017) and references wherein. Then it follows that for each miner i (see details given by Appendix B)

$$P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t - C_{\text{op}} \cdot \Sigma_{j \in \text{active}_i(t)}(t - s_j).$$

Here we also give some of their special cases which are listed below for each miner i:

Case I: When $C_{\text{op}} = 0$, we have for i at time t,

$$P_i(t) = P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t.$$

Case II: When $C_{\text{cap}}(t) = 0$, we have for i at time t,

$$P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{op}} \cdot \Sigma_{j \in \text{active}_i(t)}(t - s_j).$$

Case III: When both $C_{\text{op}} = 0$ and $C_{\text{cap}}(t) = 0$, we have that for i and at time t,

$$P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t).$$

These will be used in section below for the study and discussion on the existence of consensus equilibria for Gap Games in general.

Before the ending of this section, we also like to point out that indeed the key point which identifies our approach used in this paper different from the most of other existing literature is as follows:

1): Our study on the stability for Blockchain ecosystems is mainly based on the Profit function P_i given above by applying the concept of the consensus equilibria with the idea from game theory, and thus it allow us to deal with the general framework for Gap games, and we are able to prove the existence of the honest miners keeping "Mining Longest Chain Rules (LCR)" under a given consensus (which leads the corresponding Profit Function meeting certain conditions as required by results given in next section below), i.e., we would claim the following statements in positively:

(1): there always exists honest miners keeping "Mining Longest Chain Rules (LCR)" (though maybe with or without either "Occurring Gap Behavior, or Fork Chain" for blockchains), plus the plausibility of mining-pool attacking; and

(2): Bitcoin ecosystem always works (as the majorities of miners do not collude to break it).

2): We note that, however, many scholars (e.g., see Tsabary and Eyal (2018), Liu et al. (2019) and references wherein) follow another way by using the utility function U_i for each player (controller) i as objective to identify the impact for each miner's possible gap behavior, where the expected Profit defined by $U_i(t) := E(\text{Profit}_i)$ for each miner i.

By following this way, they transfer the choice of Gap game for miners' behaviors to a multi object optimization problem. But we all know that in general it is hard to establish the general existence result for such multi objective optimization problems, and thus algorithms are necessary introduced and used to conduct numerical analysis by the implementation of simulations as did by Tsabary and Eyal (2018), Liu et al.(2019) and others.

4 The Consensus Equilibria of Gap Games and related to the Stability of Blockchain Ecosystems

Now for a given mining gap game, where $i \in N = \{1, 2, \cdots, n\}$, without loss of generality we may assume that T_i assigned a big enough value in the real line R for time, and we define $X_i := [0, T_i]$ and $X := \prod_{i=1}^{n} X_i$. Then X_i and X are both compact and convex subsets of the real line R and R^n for $i \in N$.

Then based on the notations of a gap game introduced above, and incorporating with the profit function $P_i(t)$ for $i \in N$ at time t defined in X_i, then it is easy to see that a gap game indeed is a consensus game $CG := (N, K, (X_i, P_i)_{i \in N})$, where $N = \{1, 2, \cdots, n\}$, $K = \{1, 2, \cdots, k\}$ with the $k's$ partition $N_1, \cdots, N_2, \cdots, N_k$ of N as mentioned above.

Then we have the following general existence results for consensus equilibria of Gap Games in supporting the stability for Blochchain Ecosystems as applications of general consensus game model established in Section 2 above.

Theorem 4.1 (The Consensus Equilibria for Mining-Gap Games). For a given general Mining Gap Game (which is indeed a consensus game (in short, CG) if the profit function P_i (defined above) is concave from $[0, T_i] \mapsto R$ for each $i \in N = \{1, 2, \cdots, n\}$, then the Gap Game CG has at least one consensus equilibrium.

Proof. Note that for each $i \in N$, P_i is continuous in t, plus we assume that P_i is concave, thus P_i is continuous and concave. All assumptions of Theorem 2.1 are satisfied, then the conclusion follows by Theorem 2.1. The proof is complete.

Theorem 4.1 tells us that in general under a given consensus, if the corresponding Profit function P_i for the miner i is reasonable well (see below for each special case to be satisfied in a nature way), the idea from consensus game theory allows us to deal with the general framework for Gap games, and we are able to prove the existence of the honest miners to keep "Mining Longest Chain Rules (LCR)" under a given consensus (e.g., such as Nakamoto (2008)) which indeed answer the following question in affirmatively:

"The stability for Blockchain ecosystems is there due to the existence of the honest miners keeping "Mining Longest Chain Rules (LCR)" under a given reasonable consensus, and thus we would claim the following statements:

(1): there always exists honest miners keeping "Mining Longest Chain Rules (LCR)", plus the plausibility of mining-pool attacking; and

(2): Bitcoin ecosystem always works"

In what follows, as applications of Theorem 4.1, we have the following results by assuming the operation cost for the Gap Game's system being zero.

Theorem 4.2 (The Gap Games without Operational Cost). For a given general Gap Game with operational costs being zero, if assume the ratio function $\alpha_i(t)$ is concave in t for each $i \in N = \{1, 2, \cdots, n\}$, then the Gap Game has at least one consensus equilibrium.

Proof. For $i \in N$, by assumption that α_i is concave in t, then it follows that the second order derivative $\alpha_i^{''}$ of α_i is nonnegative. As $C_{\text{op}} = 0$, it follows that $P_i(t) = \alpha_i(t)(\lambda_0 + \lambda \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t$. Then we have that the second order derivative $P_i^{''}$ of $P_i(t)$ is no-negative, thus P_i is concave. By the fact that P_i is also continuous for $t \in X_i = [0, T_i]$. Then all assumptions of Theorem 4.1 are satisfied. Then the conclusion follows by Theorem 4.1 and the proof is complete.

Based on Theorem 4.2, we have the following discussion to illustrate one phenomenon for "No Gap" of Mining-Pool games in the practice if the system is in the case without operational cost.

Remark 4.1 (The Mining-Pool Game is Stable without Operational Cost).

By Theorem 4.2, for each miner i, its Profit function $P_i(t)$ has the following form:

$$P_i(t) = \alpha_i(t)(\lambda_0 + \lambda \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t.$$

By the fact that the term "$-C_{\mathbf{cap}} \cdot |R_i| \cdot t$" play a huge negative role for player i's income in terms of profit function P_i at time t, thus one way to reduce the loss for the system (in terms of $P_i(t)$) is to make the ratio $\alpha_i(t)$ as bigger as possible at time t. If assume miner i's computing power is m_i for $i \in N$, then one of the possible best options (strategies) for player i is to run all rigs, and thus $\text{active}_i(t) = m_i$ and so we have $\alpha_i(t) = \frac{m_i}{\Sigma_{j=1}^{k} m_j}$ for any time $t \in [0, T_i]$. Thus the ratio $\alpha_i(t)$ is independent of t and thus concave, therefor the concavity assumption is satisfies, which implies that the the system for the gap game without operational cost always has at least one equilibrium with the mining's starting time for miners at zero (thus in the situation without operational cost, the pool-games in general has no "gap" phenomenon as all miners like to start mining with starting time zero (due to the fact without any expense of the operational cost).

Second, the result discussed above by Remark 4.1 indicates that if a system is designed to mine Bitcoin with only capital cost (if the operational cost is zero), there is always exists a subgroup of miners to run the system resulting in the stability of Bitcoin Ecosystem which answer the general existence of stability for mining-pool games affirmatively, which is the basic question for mining if to follow nLongest Chain Rules (LCR) asked by people from academic to financial industries in the practice. Indeed, this is exact the case discussed by Tsabary and Eyal (2018) for the phenomenon of "Scenario One: No Mining Gap " under the assuming that "system is comprised of two miners with no operational expenses" due to a simple reason that each miner is try to increase its mining power as soon as possible to find the block without any more cost by starting at time zero (here we also illustrate the pool games of more than two miners without any gap phenomenon). Indeed, for two miners pool game, it is easy to see that both player like to increase its mining power at time zero (if no operational cost), which would lead the ratio $\alpha_1(t)$ and $\alpha_2(t)$ being $\frac{m_1}{m_1+m_2}$, and $\frac{m_2}{m_1+m_2}$, respectively to reach a general equilibrium in keeping the system running without any gap phenomenon.

When the system of mining pool games has no capital and operational cost, then we have the following general result for mining pool game without the phenomenon of the gap game behavior to occur.

Theorem 4.3 (The Ming Gap Games without Capital and Operational Cost). For a given general Gap Game with both Capital and Operational Costs are zero, if assume the ratio function $\alpha_i(t)$ is concave in t for each $i \in N = \{1, 2, \cdots, n\}$, then the mining pool game has at least one consensus equilibrium, and no phenomenon of gap game behavior.

Proof. The existence of equilibria from Theorem 4.2, and phenomenon of without gap game behavior is given by Remark 4.1. Then the proof is complete.

Remark 4.2. When both $C_{\text{op}} = 0$ and $C_{\text{cap}}(t) = 0$, by considering the Profit function $P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t)$. The best way to increase the value of $P_i(t)$ is to fully run rigs, thus it is best at the beginning to have $\alpha_i = \frac{m_i}{\Sigma_{j=1}^{k} m_j}$, where m_i is the mining power for miner $i \in \{1, 2, \cdots, n\}$. In this way, $\alpha_i(t)$ is a constat, thus all assumptions of Theorem 4.3 are satisfied, which leads the system has at least one equilibrium.

Now based on the Profit function used in Theorem 4.1, we are able to discuss the phenomenon of arbitrary mining gap without assuming the capital and operational cost for the system being zero.

Remark 4.3 (The Scenarios of Arbitrary Mining Gaps Games).

In Theorem 4.1, for each miner $i \in N = \{1, 2, \cdots, n\}$, we know that the Profit function $P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t - C_{\text{op}} \cdot \Sigma_{j \in \text{active}_{i(t)}}(t - s_j)$. Now we consider in general that the both Capital cost and Operational cost for system are not zero, then we see that the term $C_{\textbf{cap}} \cdot |R_i| \cdot t + C_{\textbf{op}} \cdot \Sigma_{j \in \textbf{active}_{i(t)}}(t - s_j)$ makes negative contribution for $P_i(t)$ at time t, but the term $\alpha_i(t)(\lambda_0 + \lambda_t \cdot t)$ makes positive contribution for $P_i(t)$ at time t. Thus the **base reward** and **fees accumulation rate** would be two important factors for miners to decide how much mining power should be used to mine Bitcoin in terms of behavior of gap games for miners to decide the starting mining time.

But the following two situations will tell us when we may observe the phenomenon of arbitrary mining gap behavior based on the high or low level of EBRR values (see definition of EBRR given in Section 3.3.3 above).

Case 1: If EBRR value is small, i.e., by assuming EBRR $\leq c$ for some constant c, then we have that $\lambda_0 \leq c \cdot \lambda_t \cdot \text{Block-Interval}$, which implies that

$$\alpha_i(t)(\lambda_0 + \lambda_t \cdot t) \leq \alpha_i(t) \cdot \lambda_t \cdot (c \cdot \text{Block-Interval} + t)$$

this means that the contribution from base ward and fees accumulation rate to $P_i(t)$ is limited, i.e., bounded above. Thus we may conclude that in general that "player i has negative utility" by the fact that as player i controls more rigs (i.e., has higher relative mining power), her per mining-rig utility is decreasing with her total mining power by the inequality above. Even though player i has higher probability to get rewarded as she controls more mining power, the increase in her expenses is more significant, resulting in lower utility. This leads the miner has the trend to run rig later (not at the beginning), i.e., the start time not at or nearby zero, which leads in the phenomenon of arbitrary mining gap.

Case 2: If EBRR value is big enough, i.e., by assuming EBRR $\geq c_1$ for some constantc_1, then we have that $\lambda_0 \geq c_1 \cdot \lambda_t \cdot \text{Block-Interval}$, which implies that

$$\alpha_i(t)(\lambda_0 + \lambda_t \cdot t) \geq \alpha_i(t) \cdot \lambda_t \cdot (c_1 \cdot \text{Block-Interval} + t)$$

this means that the contribution from base ward and fees accumulation rate to $P_i(t)$ is bounded below. Thus we have that the contribution from base ward and fees accumulation rate to $P_i(t)$ is positive by the fact as the player i controls more rigs, her per-rig utility is increasing with her total mining power. The increase in the probability to get rewarded surpasses the increase in expenses, resulting in higher utility. Thus the miner i has the trend to run rig at the very beginning of time around zero (resulting in phenomenon of no mining gap).

We like to share with readers that above trends for miners in both cases are maintained for all settings of opex and capex ratios under the consideration of BERR's high or low levels.

The second way to discuss the possible mining gap behaviors is to look at the impact to profit function P_i based on the relationship between capital and operational costs' level for system as discussed follows based on both the term $C_{\text{cap}} \cdot |R_i| \cdot t$, and the term $C_{\text{op}} \cdot \Sigma_{j \in \text{active}_i(t)}(t - s_j)$:

Case 3: For any player i relative mining power and any EBRR, the profit of player i when Capex is dominant (i.e., much higher than the level of Operational cost), thus payer i's choice of start times that are greater than zero is a better choice (leading to the phenomenon of mining gap). By doing so, the miner could reduces his expected opex as he controlled rigs are expected to be active for less time. The more rigs he controls, the more impactful this effect is. Hence, this suggests that at when opex is at play (for the case operational cost is in the middle or higher level), by taking mining gap would be a better option in general.

Case 4: But for the other case, i.e., when the level of Capex cost is not much higher than operational cost, the miner may not have mining gap behavior in the practice as taking early time to run rig may lead find the block early and thus less cost contributed by operational cost (as the term $C_{\text{cap}} \cdot |R_i| \cdot t$ may not a big amount comparing with the amount $C_{\text{op}} \cdot |R_i| \cdot t$) and by the following inequality:

$$C_{\text{op}} \cdot |\text{active}_i(t)| \min_{j \in \text{active}_i(t)} \{(t - s_j\}) \leq C_{\text{op}} \cdot |\text{active}_i(t)| \cdot t \leq C_{\text{op}} \cdot |R_i| \cdot t.$$

But maybe the behavior of the mining gap would happen if capital cost is no much less than the operational cost.

The discussion above with the illustrations by Case 3 and Case 4 using the profit function P_i for miner i show that the operational costs are also a major factor to cause the phenomenon of mining gaps for system. This is actually true observations and confirmed with numerical simulations given by Tsabary and Eyal (2018).

Putting all together, for the behaviors of gap games, they are basically caused by three factors which are 1):**base reward** and **fees accumulation rate**; 2): the operational cost, and also capital cost level; and 3): the mining power.

Thus as the applications of BERR level, we would have the following expectation for the case study of Bitcon in long term by looking at future.

Remark 4.4 (The Case Study for the Bitcoin).

By following Tsabary and Eyal (2018), we give a brief discussion for Bitcion ten years from now based on the Profit function $P_i(t)$ for the miner i at time t.

By thinking the Bitcoin becomes prone to the undesired effects of mining gaps, thus there are many operational cryptocurrency systems, all vary in minting, fees, market cap, and expenses. Given such parameters for any cryptocurrency, a similar estimation can be performed using the model studied here and thus we present a case study of Bitcoin as followed with illustration by Theorem 4.1.

In Bitcoin today, there are around 7 mining pools (see [9]-[11])) controlling about 85% of the mining power, while the rest is divided among many smaller mining pools. Although they vary in size, we approximate that situation by assuming 8 equal size miners.

By assuming long time from today (for example, around 10 years), we assume that EBRR is round 1, which may be required to maintain a small gap. Currently, the rewards from minting and fees are $B12.5$ and about $B1$, respectively. Therefore currently EBRR $\approx$

12.5, so gaps are not profitable. However, in about ten years the minting reward drop which may lead EBRR around around 1. This means that the factor " λ_t " plays a bigger role by representing the time vale of the positive term $\alpha_i(t)(\lambda_0 + \lambda_t \cdot t)$ as by maintaining the cost term $C_{\mathbf{cap}} \cdot |R_i| \cdot t + C_{\mathbf{op}} \cdot \Sigma_{j \in \mathbf{active}_i(t)}(t - s_j)$ reasonable small, thus the term $P_i(t)$ is positive when time t is long enough in future. The phenomenon of mining gaps for Bitcoin in long term (around ten years from now by assuming the EBRR is around 1) is also illustrated by the analysis of Remark 4.3.

Before the end of this paper, we like to mention that based on a new notion called "Consensus Game (CG)" with motivation from the mechanism design of blockchain economy under the consensus incentives from Bitcoin ecosystems, we first establish a general existence result for the consensus equilibria of general gap gams for miners by using their profit functions directly. In applications, we discuss the general phenomenon of mining gaps for mining-pools, and by assuming that ten years from now, with assumption of EBRR being around one, we show that though the behavior of gap game for mining-pools of Bitcoin economics would happen (by the discussion of Remark 4.3), but the blockchain as a platform for Bitcoin ecosystem is "stable" in the sense that there are still honest miners to mine blocks by following "mining LCR" in the practice (by Theorem 4.1).

We wish to point out that the study on the existence of Mining Gap games and related stability for mining-pools games by applying consensus games show that the concept of consensus equilibria would play a key role for the development of fundamental theory for consensus economics. Indeed, the concept of consensus games can also be used to establish the general fundamental results in supporting existence and related stability for mining-pool games of Bitcoin economics, too.

5 Conclusion

By incorporating both cooperative and noncooperative behaviors in game theory for the Mining Pool Game for Bitcoin ecosystems under the mechanism design of the blockchain platform by following the general framework of Nakamoto consensus principle (2008), it is nature to introduce a new concept called "*consensus game*". This new notion allows us to analyze the choices of strategies in which there exist cooperative and noncooperative behaviors in different situations, which can be used to explain the stable for mining gap games by using one new concept called "Consensus Games (CG)" . In order to do so, we first give an outline how the general existence for consensus equilibria is formulated, and used to explain the stable in the sense for the existence of consensus equilibria of mining gap games for Bitcoin, we then establish a general existence result for the consensus equilibria of general mining gap games by using the profit functions as payoff functions. As applications, the results are used to illustrate some specifical issues and problems on the study of mining pool-games with possible impacts due to miners' gap behaviors, and also used to explain scenarios for different phenomenons of mining gap behavior embedded in Blockchain Ecosystems. Our study on the existence and the explanation for the stability of mining gap game for Blockchain ecosystems shows that the concept of consensus equilibria may play a important role for the development of fundamental theory for consensus economics.

By comparing with the traditional cooperative and noncooperative game, it seems that our concept for consensus game is a natural extension for consensus economy, especially under the framework of Bitcoin ecosystem associated with consensus incentives in Bitcoin ecosystems (in terms of Nakamoto′s consensus protocol as one example), our study in this this paper shows that it may be used to lay the foundation for consensus economics.

We conclude that the existence results of consensus equilibria for consensus games defined in this paper are useful and should provide the base for the study of consensus economics under the framework of Blockchain in fintech as shown by the discussion above. Furthering the study on different situations related to smart contracts for different kinds of digital business activities under the Blackchain with associated consensus' incentives (called "blackchain economy") should be one of the most important things in era of big data. We also note that recently some issue and problems related to topics in fintech have been studied by a number of scholars, for example, the dynamic equilibria under blockchain disruption was initially discussed by Cong and He (2019), topics surrounding blockchain-based accounting and assurance was outlined by Dai and Vasarhelyi (2017), and other related areas of interest issues were discussed by Narayanan et al. (2016). Moreover a number of issues and problems in Finteh have been recently addressed by Goldstein et al.(2019), Chiu and Koeppl (2019), Foley et al. (2019), Fuster et al.(2019), Tang (2019), Vallee and Zeng (2019), D′Acunto et al.(2019), Zhu (2019), Chen et al.(2019), Di et al.(2019) and references wherein.

Finally, we like to share with readers that as our goal in this paper is to show how the new notion called "Consensus Equilibria" for Mining-Pool games can be used to study the impact for the stability for Blockchain ecosystems when miners from mining-pool may have gap behaviors, the general framework of Mining-Pool Games is assumed to be with the homogeneity for cost structures and with symmetry of information for all miners. Indeed, by incorporating both notions of "consensus equilibria" and "Markov equilibrium" concept, we can also study the impact for the stability by miners' Gap behaviors under the assumption of the "heterogeneity for the cost structures and with asymmetry of the information ” for miners in the Mining-Pool games, and this is our next work to do.

6 Acknowledgement

This research is supported in part by NSF of China under Nos. U181140004 and 11501349.

References

[1] Askoura, Y. 2011. The weak-core of a game in normal form with a continuum of players.2011. Journal of Mathematical Economics 47(1):43-47.

[2] Askoura, Y., M. Sbihi, and H. Tikobaini. 2013. The exante $\alpha-$core for normal form games with uncertainty. Journal of Mathematical Economics 49(2):157-162.

[3] Aumann, R.J. 1961. The core of a cooperative game without sidepayments. Transactions of the American Mathematical Society 98:539–552.

[4] Badertscher, C., U. Maurer, D. Tschudi, and V. Zikas. 2017. Bitcoin as a transaction ledger: A composable treatment.In: Katz, F., Shacham, H. (eds.) CRYPTO 2017, Part I, LNCS, vol. 10401. pp 324 - 356. Springer, Heidelberg.

[5] Badertscher, C., J. Garay, U. Maurer, D. Tschudi, and V. Zikas. 2018. But why does it work? A rational protocol design treatment of bitcoin. Advances in cryptology−EUROCRYPT 2018, Part II, Lecture Notes in Comput. Sci., vol. 10821. pp.34 - 65. Springer, Cham (2018).

[6] Bahackm L. 2013. Theoretical Bitcoin Attacks with less than Half of the Computational Power. Technical Report abs/1312.7013, CoRR.

[7] Biais, B., C. Bisire, M. Bouvard, and C. Casamatta. 2019. The blockchain folk theorem. Review of Financial Studies 32(5): 1662-1715.

[8] Binns, W. 2018. How do I calculate my transaction fee? https://support.earn.com/digital-currency/bitcoin-transactions-and-fees/how-do-i-calculate-my-tracsavtion-fee (2018).

[9] Blockchain.info. 2018a. Bitcoin Market Capitalization. http://blockchain.info/charts/market-cap, retrieved Feb.(2018).

[10] Blockchain.info. 2018b. Bitcoin Mining Pools. https://blockchain.info/pools, retrieved May (2018).

[11] Blockchain.info. 2018c. Transaction Fees. https://blockchain.info/charts/transaction-fees, retrieved Feb.(2018).

[12] Bonneau, J., A. Miller, J. Clark, A. Narayanan, A. Kroll, and E. Felten. 2015. Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In: Proceedings of the 36th IEEE Symposium on Security and Privacy, San Jose, California, USA (May 18-20, 2015).

[13] Border, K.C. 1984. A core existence theorem for games without ordered preferences. Econometrica 52(6): 1537-1542.

[14] Browne, R. 2017. The cheapest and most expensive countries to mine bitcoin (2017). https://www.cnbc.com/2018/02/15/the-cheapest-and-most-expensive-countries-to-mine-bitcoin.html.

[15] Carlsten, M., H. Kalodner, S.M. Weinberg, and A. Narayanan. 2016. On the instability of Bitcoin without the block reward. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ACM, pp.154 - 167, Vienna, Austria (October 24 - 28, 2016).

[16] Chen, M., Q. Wu, and B. Yang. 2019. How valuable is FinTech innovation? Review of Financial Studies 32(5):2062-2106.

[17] Chiu, J., and T. Koeppl. 2019. Blockchain-based settlement for asset trading. Review of Financial Studies 32(5): 1716-1753.

[18] Cong, L.W., and Z. He. 2019. Blockchain disruption and smart contracts. Review of Financial Studies 32(5): 1754-1797.

[19] D'Acunto, F., N. Prabhala, and A.G. Rossi. 2019. The promises and pitfalls of Robo-Advising. Review of Financial Studies 32(5): 1983-2020.

[20] Dai, J., and M.A. Vasarhelyi. 2017. Toward blockchain-based accounting and assurance, J. Information Systems 31:5-21.

[21] Di, L., Z. Yang, and George X. Yuan. 2019. The consensus games for consensus economics under the framework of Blockchain in fintech. In: Li, D.F.(eds).Communications in Computer and Information Science, Vol. 1082, pp. 1

- 26. 3rd East Asia Game Theory International Conference (March 7 - 9, 2019, Fuzhou University, Fujian, China). Springer, Singapore (2019).

[22] Digiconomist.net. 2017. A Deep Dive in a Real-World Bitcoin Mine. https://digiconomist.net/deep-dive-real-world-bitcoin-mine (2017).

[23] Digiconomist.net. 2018a. Bitcoin Energy Consumption Index. https://digiconomist.net/bitcoin-energy-consumption (2018).

[24] Digiconomist.net. 2018b. Ethereum Energy Consumption Index. https://digiconomist.net/ethereum-energy-consumption (2018).

[25] Earn.com. 2018. Predicting Bitcoin Fees For Transactions. https://bitcoinfees.earn.com/(2018).

[26] Eyal, I. 2015. The Miners Dilemma. In: Proceedings of the 36th IEEE Symposium on Security and Privacy, San Jose, California, USA (May 18-20, 2015).

[27] Eyal,I., E. G. Sirer 2014. Majority is not enough: Bitcoin mining is vulnerable. In: Proceedings of the 18th International Conference on Financial Cryptography and Data Security, FC′14, pp. 436 - 454. Springer, Berlin Heidelberg.

[28] Florenzano, M. 1989. On the nonemptiness of the core of a coalitional production economy without ordered preferences. Journal of Mathematical Analysis and Applications 141:484-490.

[29] Foley, S., J.R. Karlsen, and T. Putnins. 2019. Sex, Drugs, and Bitcoin: How much illegal activity is financed through Cryptocurrencies? Review of Financial Studies 32(5): 1798-1853.

[30] Fuster, A., M. Plosser, S. Schnabl, and J. Vickery. 2019. The Role of Technology in Mortgage Lending, Review of Financial Studies 32(5): 1854-1899.

[31] Garay, J.A., J. Katz, B. Tackmann, and V. Zikas. 2015. How fair is your protocol? A utility-based approach to protocol optimality. In: Georgiou, G., Spirakis, P.G. (eds). The 34th ACM PODC, ACM. pp. 281 - 290. (July, 2015).

[32] Garay, J.A., A. Kiayias, and N. Leonardos. 2014. The Bitcoin Backbone Protocol: Analysis and Applications. Cryptology ePrint Archive, Report 2014/765.

[33] Garay, J.A., A. Kiayias, and N. Leonardos. 2015. The bitcoin backbone protocol: Analysis and applications. In: Oswald, E., Fischlin, M. (eds). EUROCRYPT 2015, Part II, LNCS, vol.9057 , pp. 281 - 310. Springer, Heidelberg (April 2015).

[34] Garay, J.A., A. Kiayias, and N. Leonardos. 2017. The bitcoin backbone protocol with chains of variable difficulty. In: Katz, j., Shacham, H (eds). CRYPTO 2017, Part I, LNCS, vol. 10401. pp. 291 - 323. Springer, Heidelberg (August 2017).

[35] Goldstein,I., W. Jiang, and G. Karolyi. 2019. To FinTech and beyond. Review of Financial Studies 32(5): 1647 - 1661.

[36] Ichiishi, T. 1981. A social coalitional equilibrium existence lemma. Econometrica 49: 369–377.

[37] Kajii, A. 1992. A generalization of Scarf's theorem: an $\alpha-$core existence theorem without transitivity or completeness. Journal of Economic Theory 56:194–205.

[38] Khatwani, S. 2018. Ethereum: Ether, Ether Gas, Gas Limit, Gas Price and Fees. https://coinsutra.com/ethereum-gas-limit-gas-price-fees/ (2018).

[39] Kiayias, A., E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis. 2016. Blockchain mining games. In: 2016 ACM Conference on Economics and Computation, Maastricht, The Netherlands (July 24-28, 2016).

[40] Kroll, J., I. Davey, and E. Felten. 2013. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: Proceedings of The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Georgetown University, Washington DC, USA (June 11-12, 2013).

[41] Kwon, Y., D.Kim, Y. Son, E. Vasserman, and Y. Kim. 2017. Be selfish and avoid Dilemmas: Fork after withholding (FAW) attacks on Bitcoin. In 2017 ACM CCS$'$17, Oct.30 - Nov.3, 2017, Dallas, TX, USA. 2017 ACM. ISBN 978-1-4503-4946-8/17/10 (DOI: http://dx.doi.org/10.1145/3133956.3134019).

[42] Lefebvre, I. 2001. An alternative proof of the nonemptiness of the private core. Economic Theory 18(2): 275–291.

[43] Liu, Y., J. Ke, Q. Xu, H. Jiang, and H. Wang. 2019. Decentralization is vulnerable under the Gap game. IEEE Access 7: 90999-91008 (2019).

[44] Malkin, S. 2018. Cheapest Places Mining Bitcoin. https://cryptocurrencynews.com/daily-news/cryptocurrency-mining/cheapest-places-mining-bitcoin/ (2018).

[45] Martins-da-Rocha, V.F., and N. Yannelis. 2011. Nonemptiness of the alpha core. Working paper. Manchester School of Social Sciences, University of Manchester.

[46] Miller, A. 2013. Feather-forks: enforcing a blacklist with sub-50% hash power. bitcointalk.org (October 2013).

[47] Miller, A., and J.J. LaViola Jr. 2014. Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin.

[48] Möser, M., Böhme, R. 2015. Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees. In Financial Cryptography and Data Security, Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 19 - 33.

[49] Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system (/http://bitcoin.org/bitcoin.pdf).

[50] Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction Hardcover, Princeton University Press.

[51] Nayak, K., Kumar, S., Miller, A., and E. Shi. 2015. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. IACR Cryptology ePrint Archive 2015 (2015), 796. http://eprint.iacr.org/2015/796 (2015).

[52] Noguchi, M.2018. Alpha cores of games with nonatomic asymmetric information. Journal of Mathematical Economics 75: 1-12.

[53] Nyumbayire, C. 2017. The Nakamoto Consensus (https://www.interlogica.it/en/insight-en/nakamoto-consensus). Insight, Interlogica.

[54] Pass, R., L. Seeman, and A. Shelat. 2017. Analysis of the blockchain protocol in asynchronous networks. In: Coron, J., Nielsen, J.B. (eds). EUROCRYPT 2017, Part II, LNCS, vol. 10211. pp. 643 - 673. Springer, Heidelberg.

[55] Rosenfeld, M. 2011. Analysis of Bitcoin pooled mining reward systems. arXiv preprint arXiv: 1112. 4980.

[56] Saleh, F. 2020. Blockchain Without Waste: Proof-of-Stake (January 15, 2020). Available at SSRN: https://ssrn.com/abstract=3183935 or http://dx.doi.org/10.2139/ssrn.3183935

[57] Sapirstein, A., Y. Sompolinsky, and A. Zohar. 2016. Optimal selfish mining strategies in bitcoin. In: Grossklags, J., Preneel, B.(Eds.) Financial Cryptography 2017, LNCS, vol. 9603. pp. 515 - 532. The 20th International Conference (FC 2016, Christ Church, Barbados, February 22- 26, 2016).

[58] Scarf, H.E. 1971. On the existence of a cooperative solution for a general class of n-person games. Journal of Economic Theory 3: 169 - 181.

[59] Schrijvers, O., J. Bonneau, D. Boneh, and T. Roughgarden. 2016. Incentive compatibility of Bitcoin mining pool reward functions. In: J. Grossklags, J., Preneel, B.(Eds.) Financial Cryptography 2017, LNCS, vol. 9603. pp. 477 - 498. The 20th International Conference (FC 2016, Christ Church, Barbados, February 22- 26, 2016).

[60] Shafer, W., and H. Sonnenschein. 1975. Equilibrium in abstract economies without ordered preferences. Journal of Mathematical Economics 2: 345-348.

[61] Tang, H. 2019. Peer-to-Peer lenders versus banks: substitutes or complements? Review of Financial Studies 32(5): 1900-1938.

[62] Tsabary, I., and I. Eyal. 2018. The gap game. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security (CCS′ 18), 713-728.

[63] Tuwiner, J. 2017. Bitcoin Mining Hardware. https://www.buybitcoinworldwide.com/mining/hardware/ (2017).

[64] Uyanik, M. 2015. On the nonemptiness of the $\alpha-$core of discontinuous games: Transferable and nontransferable utilities. Journal of Economic Theory 158: 213-231.

[65] Vallee, B., and Y. Zeng. 2019. Marketplace Lending: A New Banking Paradigm? Review of Financial Studies 32(5): 1939 - 1982.

[66] Wang, C. 2017. A Visit to a Bitcoin Mining Farm in Sichuan, China Reveals Troubles Beyond Regulation. https://news.bitcoin.com/a-visit-to-a-bitcoin-mining-farm-in-sichuan-china-reveals-troubles-beyond-regulation/ (2017)

[67] Weber, S. 1981. Some results on the weak core of a non-side-payment game with infinitely many players. Journal of Mathematical Economics 8: 101 - 111.

[68] Yannelis, N.C., and N.D. Prabhakar. 1983. Existence of maximal elements and equilibria in linear topological spaces. Journal of Mathematical Economics 12: 233-245.

[69] Yang, Z., and X.Z. Yuan. 2019. Some generalizations of Zhao's theorem: hybrid solutions and weak hybrid solutions for games with nonordered preferences. Journal of Mathematical Economics 84: 94 - 100.

[70] Yuan, X.Z. 1999. The study of equilibria for abstract economies in topological vector spaces-a unified approach. Nonlinear Aanalysis 37: 409-430.

[71] Zhao, J. 1992. The hybrid solutions of an N-person game. Games and Economic Behavior 4: 145-160.

[72] Zhao, J. 1996. The hybrid equilibria and core selection in exchange economies with externalities. Journal of Mathematical Economics 26(4): 387 - 407.

[73] Zhu, C. 2019. Big data as a governance mechanism, Review of Financial Studies 32(5): 2021-2061.

Appendix A: The Consensus Games

By following the notations from Section 2, we now recall some results from Yang and Yuan (2019). The following is the consensus game's version due to Theorem 3.1 of Yang and Yuan (2019) (see also Theorem 3.1 of Di et al.(2019)).

Theorem A.1. *Suppose that a consensus game*

$$CG = (N, p, (X(t))_{t \in N}, P)$$

satisfies the following conditions:

(i) N is a finite set;

(ii) for each $t \in N$, $X(t)$ is a nonempty convex compact subset of R^{m_t};

(iii) for each $t \in N$, $P(t, \cdot)$ is convex-valued with open graph in $X \times X$, and $x \notin P(t, x)$ for any $x \in X$.

Then there exists at least a consensus equilibrium of CG.

Yang and Yuan (2019) next gave an infinite dimensional version of Theorem A.1 (by Theorem 3.2 of Yang and Yuan (2019)), here we state it by using the concept of consensus games.

Theorem A.2. *Suppose that a consensus game*

$$CG = (N, p, (X(t))_{t\in N}, P)$$

satisfies the following conditions:

(i) N is a finite set;

(ii) for each $t \in N$, $X(t)$ is a nonempty convex compact subset of a Hausdorff topological vector space $E(t)$;

(iii) for each $t \in N$, $P(t, \cdot)$ is convex-valued with open graph in $X \times X$ and $x \notin P(t, x)$ for any $x \in X$.

Then there exists at least a consensus equilibrium of CG.

As an application of Theorem A.2, we have the following corollary which is indeed an extension of Theorem A.1 into topological vector spaces.

Corollary A.1. *Suppose that a normal-form game with a partition*

$$G = (N, p, (X_i, u_i)_{i\in N})$$

satisfies the following conditions:

(i) N is a finite set;

(ii) for each $i \in N$, X_i is a nonempty convex compact subset of a Hausdorff topological vector space E_i;

(iii) for each $i \in N$, u_i is continuous and quasiconcave on X.

Then there exists at least a hybrid solution of G (thus the consensus equilibrium of consensus game G).

Appendix B: The Profit Function of Mining Gap Games

For a given miner $i = 1, 2, \cdots, k$, assume a single rig $j \in R_i$ with start time s_j. We denote the time this rig requires for finding a block as a random variable B_j. Recall that the rate of a single rig is $\mu(\hat{s})$, which is set by the protocol. The value of B_j is drawn from the shifted exponential distribution, with a shift of s_i and rate $\mu(\hat{(s)})$.

In order to find the profit (and associated utility) function for each player i of Gap Games at time t, we start by analyzing the block finding time's probability distribution. This is a function of the players$'$ selection of start times. We model the block finding time as a random variable denoted by B with cumulative distribution function (CDF) denoted by $F_B(t; \hat{s}, \mu(\hat{s}))$, and probability density function (PDF) denoted by $f_B(t; \hat{s}, \mu(\hat{s}))$, respectively. Then the PDF of B_i is given by

$$f_{B_j} = \begin{cases} 0 & t \leq s_j \\ \mu(\hat{s}) \cdot \exp(-\mu(\hat{s})(t - s_j)) & t > s_j \end{cases}$$

and its CDF is given by

$$F_{B_j} = \begin{cases} 0 & t \leq s_j \\ 1 - \mu(\hat{s}) \cdot \exp(-\mu(\hat{s})(t - s_j)) & t > s_j. \end{cases}$$

By the fact that $F_{B_j}(t; s_j, \mu(\hat{s})) = Pr(t \geq B_j) = 1 - Pr((t \leq B_j)$, it follows that

$$Pr(t \leq B_j) = \begin{cases} 1 & t \leq s_j \\ \exp(-\mu(\hat{s})(t - s_j)) & t > s_j. \end{cases}$$

As all rigs are competing on finding the next block, the rig that finds the next block first is the rig with the minimal value of B_j, thus the time required for finding the next block is given by the following stop time process B defined as a stop time process:

$$B := \min_{j \in \{1,2,\cdots,k\}} B_j.$$

For any time t and any player i, the active set $\text{active}_i(t)$ is defined as

$$\text{active}_i(t) := \{j \in R_i : s_j \leq t\} \text{ and we also define } \text{active}(t) := \cup_{i=1}^{k} R_i.$$

The probability that none of the rigs have found a block by time t is denoted by $Pr(t \leq B\}$, which is indeed the product of $Pr(t \leq B_j\}$ (as all rigs are independent of another one) and thus we have

$$Pr(t \leq B) = \cap_{j \in \{1,2,\cdots,n\}} Pr(t \leq B_j) = \prod_{j=1}^{n} Pr(t \leq B_j) = \exp(-\mu(\hat{s}) \cdot \Sigma_{j \in \text{active}(t)}(t - s_j)).$$

Its corresponding CDF is

$$F_B(t; \hat{s}, \mu(\hat{s})) = 1 - Pr(t \leq B) = 1 - \exp(-\mu(\hat{s})) \cdot \Sigma_{j \in \text{active}(t)}(t - s_j)),$$

and corresponding PDF is

$$f_B(t; \hat{s}, \mu(\hat{s}))) = \mu(\hat{s})) \cdot |\text{active}(t)| \exp(-\mu(\hat{s})) \cdot \Sigma_{j \in \text{active}(t)}(t - s_j)).$$

Recall that once a rig is turned on, the time it requires to find a block is drawn from the exponential distribution. The exponential distribution is memoryless, meaning the time that passed does not affect the chances of a rig to find the block. Since the rate parameter $\mu(\hat{s})$ is shared among all rigs, at any given time all the active rigs have the same chance to find the block, regardless of how much time they had been active for already. By the fact that the set of active rigs at the time the block is found active(t), the probability of a specific active rig to find the block is one divided by the total number of active rigs. Note that since the block was found at time t, then there exists $j \in \{1, 2, \cdots, k\}$ such that $s_j \leq t$ and thus $|\text{active}(t)| > 0$. As Players may control many rigs, so the probability that player i controls the rig that found the block is he number of her controlled active rigs divided by the total number of active rigs. We denote the ratio of player i's active rigs out of all the active rigs at time t by $\alpha_i(t)$ at time t defined by

$$\alpha_i(t) := \frac{|\text{active}_i(t)|}{|\text{active}(t)|}.$$

It is clear that the ratio $\alpha_i(t)$ is continuous in t, and is also the expected factor of player i's portion of the total reward. Thus for a block is found at time t, the expected income (denoted by $\text{E}(\text{Income}_i|B = t)$) of player i at time t is

$$\text{E}(\text{Income}_i|B = t) = \alpha_i(t) \cdot (\lambda_0 + \lambda_t \cdot t).$$

We recall that players have two kind of expenses (see also Tsabary and Eyal (2018)): The first one called "Capex", would be explained for the capital cost such as for "owning a rig"; and the second one called "Open", for example, which would be explained for the operation cost such as for "keeping a rig active". As Capex applies for all rigs controlled by the player, whether they are turned on or not, it follows for each rig, the capex it imposes by time t is the $C_{\text{cap}} \cdot t$.

On the other hand, recall that R_j is the set of rig indices that player j controls, which totals with $|R_j|$ rigs, thus the total Capex of player j at time t are $C_{\text{cap}} \cdot |R_j| \cdot t$.

Considering the Opex applies only for active rigs, for each active rig, the expenses it imposes by time t is the product of C_{op} and the time duration this rig is turned on already: At time t, the active rig j with s_j has been active for the time of $t - s_j$. Then the expected expenses (denoted by $E(\text{Expense}_i|B = t)$) of player i at time t is given by

$$E(\text{Expense}_i|B = t) := C_{\text{cap}} \cdot |R_i| \cot t + C_{\text{op}} \cdot \Sigma_{j \in \text{active}_{i(t)}}(t - s_j).$$

Now for a given miner (player, or saying, controller) i at time t, we can define its Profit Function P_i through the expected income function and expense function as given below:

$$P_i(t) := E(\text{profit}_i|B = t) = E(\text{Income}_i|B = t) - E(\text{Expensive}_i|B = t)$$

where $E(\text{Income}_i|B = t)$ and $E(\text{Expensive}_i|B = t)$ are expected income and expenses at time t for a given Gap Game. As discussed above, in general we assume the reward functuon is given by the following form

$$E(\text{Income}_i|B = t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t)$$

and

$$E(\text{Expensive}_i|B = t) = C_{\text{cap}} \cdot |R_i| \cdot t + C_{\text{op}} \cdot \Sigma_{s \in \text{active}_i(t)}(t - s).$$

Thus it follows that

$$P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t - C_{\text{op}} \cdot \Sigma_{j \in \text{active}_i(t)}(t - s_j).$$

The same as did by Tsabary and Eyal (2018), we can also define the utility function U_i (which is the expectation of $P_i(t)$) as:

$$U_i := E(P_i(t)) = E(E(\text{Profit}_i|B = t)) = \int_{-\infty}^{+\infty} (E(\text{Profit}_i|B = t) \cdot f_B(t; \hat{s}, \mu(\hat{s}))dt.$$

Then the utility function U_i for the player (controller) i is given by

$$U_i(t) = E(\text{Profit}_i) = E(E(\text{profit}_i|B = t)) =$$

$$\int_{-\infty}^{+\infty} \{\alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t - C_{\text{op}} \cdot \Sigma_{j \in \text{active}_i(t)}(t - s_j)\} \cdot f_B(t, \hat{s}, \mu(\hat{s})))dt$$

$$= \int_{-\infty}^{+\infty} \{\alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t - C_{\text{op}} \cdot \Sigma_{j \in \text{active}_i(t)}(t - s_j)\} \cdot$$

$$\{\mu(\hat{s}) \cdot |\text{active(t)}| \cdot \exp(-\mu(\hat{s}) \cdot \Sigma_{j \in \text{active(t)}}(t - s_j))\}dt.$$

Case I: When $C_{\text{op}} = 0$, we have for i at time t,

$$P_i(t) = P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t$$

and

$$U_i = \int_{-\infty}^{+\infty} \{\alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{cap}} \cdot |R_i| \cdot t\} \cdot \{\mu(\hat{s}) \cdot |\text{active(t)}| \cdot \exp(-\mu(\hat{s}) \cdot \Sigma_{j \in \text{active(t)}}(t - s_j))\}dt.$$

Case II: When $C_{\text{cap}}(t) = 0$, we have for i at time t,

$$P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t) - C_{\text{op}} \cdot \Sigma_{j \in \text{active}_{i(t)}}(t - s_j)$$

and

$$U_i(t) = \int_{-\infty}^{+\infty} \{\alpha_i(t)(\lambda_0+\lambda_t \cdot t) - C_{\text{op}} \cdot \Sigma_{j \in \text{active}_{i(t)}}(t-s_j)\} \cdot \{\mu(\hat{s}) \cdot |\text{active(t)}| \cdot \exp(-\mu(\hat{s}) \cdot \Sigma_{j \in \text{active(t)}}(t-s_j))\} dt$$

Case III: When both $C_{\text{op}} = 0$ and $C_{\text{cap}}(t) = 0$, we have that for i and at time t,

$$P_i(t) = \alpha_i(t)(\lambda_0 + \lambda_t \cdot t)$$

and

$$U_i = \int_{-\infty}^{+\infty} \alpha_i(t)(\lambda_0 + \lambda_t \cdot t) \cdot \{\mu(\hat{s}) \cdot |\text{active(t)}| \cdot \exp(-\mu(\hat{s}) \cdot \Sigma_{j \in \text{active(t)}}(t - s_j))\} dt.$$